

A SPECIAL REPORT:

Top Ten Myths of Information Security

Created June 2007

Phone: 773.868.4381

Fax: 773.913.6217

www.en-terpret.com

3642 N Magnolia, Suite 2

Chicago, Illinois 60613 USA

Associated Worldwide with JHI
www.jhi.com



INTRODUCTION

Information is perhaps the most important asset for modern business. The future of your enterprise depends on your ability to collect, process, share and store vast amounts of data. And yet, most companies fail miserably to protect even their most valuable information resources. Someone could be reading your confidential sales forecasts right now, or using your social security number to drain your savings account. Sound far-fetched? Just read the news. In the past year alone, a laptop computer containing confidential information about 26.5 million current and former members of the American military was stolen from the home of a private contractor. Three men were indicted for trying to sell Coke's most closely guarded trade secrets to the highest bidder. If the United States government and the Coca-Cola Company can't protect themselves, what chance do you have?

Cyber criminals prowl the web almost unchecked, like masked gunslingers in a digital Wild West. E-mails can be hijacked and databases broken into like an open bank vault. Entire IT systems can be compromised, leaving your company at the mercy of the information bandits. The time, money and effort you invested to gain a critical competitive edge can be lost with a single keystroke. And imagine the irreparable damage to your hard-earned reputation if critical data were lost or stolen from your organization.

INSIDE THIS REPORT:

Password protection is an oxymoron

Any hacker can break through quicker than you can remember your username..... p. 3

E-mail is an open book

Why your most sensitive messages might have a bigger audience than Stephen King's last novel p. 4

Kids are a security risk!

The hottest shareware products your kids can't live without are a threat to your home computer and your business p. 5

Don't rely on firewalls

They are designed to protect you from external threats, but the biggest problems are right at home p. 6

A bad day "phishing"

beats a good day at work
Find out about a scam that could cost you a lot of money and your peace of mind p. 7

Coffee jitters

If you bring your laptop to Starbucks, you might leave with more than just a double-mocha latte p. 8

Don't turn your back

The information on your computer is worth a lot more than the machine itself p. 9





Part of the problem is that even the most informed, intelligent and thoughtful business people can be lulled into a **false sense of security** by misleading or incomplete assumptions about information security. We want to believe we are safe so we convince ourselves that we are, even though all of the evidence suggests otherwise. An entire mythology has grown up around information security, but unlike the stories of Billy the Kid or the Gunfight at the OK Corral, these myths can be dangerous. Taking only half-measures to protect your information assets might be worse than doing nothing at all. The following is a list of the **Top Ten Myths of Information Security** – and how you can avoid them.

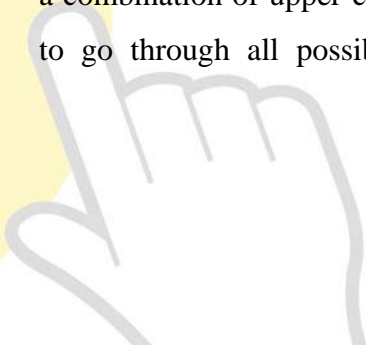
1. MY COMPUTER HAS A PASSWORD, SO MY DATA IS SECURE.

Passwords are the most common information security features on modern computers. If you have assigned a Windows password to your computer, for example, you must provide that password and a username before the system will boot up. This is a good start, but not nearly enough to ensure complete security. There are many ways for unauthorized users to bypass the password barrier.

A strong password has at least eight characters, including at least one number, and both upper and lower-case letters.

Most of us choose a password that reflects some aspect of our professional or personal lives. An individual's password might have something to do with a favorite hobby or job title – *catperson*, for example, or *bossman*. If the bad guys know a little bit about you, chances are they will eventually be able to crack your password. There are certain steps you can take, however, to make your password less vulnerable.

A **strong password** has at least eight characters, including at least one number, and a combination of upper-case and lower-case letters. The bad guys won't have time to go through all possible combinations – in fact, it is nearly mathematically





impossible for even the most sophisticated super-computer to run all possible variations in a given period of time.

And be sure to use passwords wherever possible. There is an administrator account on your computer, for example, which controls all facets of its operation. Windows does not require a password for this account and most people never assign one. **It's like locking the doors to your house and giving the key to a complete stranger.**

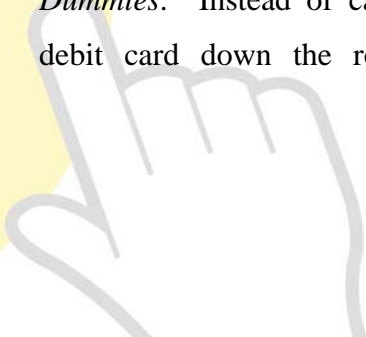
Even with a strict password protocol, however, there is no way to completely protect your data if you are careless about how you store it. The data on a disk, flash drive, or CD, for example, is not encrypted and the disk can be easily removed and placed in another machine, giving someone else full access to all of your most sensitive files.

2. E-MAIL IS A GOOD WAY TO SEND SENSITIVE INFORMATION BECAUSE IT IS DELIVERED DIRECTLY TO THE RECIPIENT'S MAILBOX.

Actually, a single **e-mail message** will be transferred between *dozens* or even *hundreds* of other public systems before it reaches its intended destination. Each stop along the way gives the bad guys another opportunity to intercept your message. Your most private and confidential correspondence might have more readers than Stephen King's last novel.

One of the great benefits of e-mail is that it can be accessed by many different systems. If you have a PC and your colleague has a Mac, you can swap e-mails without any problem. Unfortunately, this means that e-mail must be transmitted in standard formats that are easily accessible to anyone with a copy of *Computer Hacking for Dummies*. Instead of cash, think about passing your debit card down the row at a baseball game and

Never send confidential or sensitive information by e-mail. Imagine that everyone in the world is reading your e-mail, because they probably are.





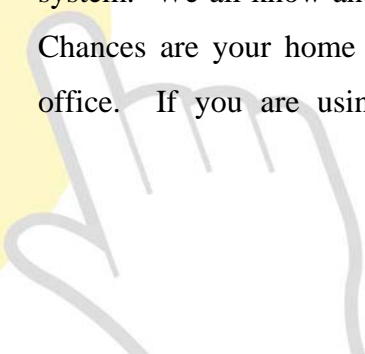
whispering your PIN number to each person along the way so the vendor can process the transaction. Who would take such a risk? You should **never** send confidential or sensitive information by e-mail. Imagine that everybody in the world is reading your e-mail messages, because they probably are. If sending critical information by e-mail is a must, at least beef up your security system and take whatever steps are necessary to protect your confidentiality. There is a good reason why most diaries come with a lock and key.

3. MY COMPANY USES A VIRTUAL PRIVATE NETWORK WHICH SECURELY CONNECTS MY HOME COMPUTER TO THE OFFICE SYSTEM – THIS MEANS I CAN WORK FROM HOME WITHOUT ANY PROBLEMS.

Like a password, a *Virtual Private Network* (VPN) is an essential security precaution. It undoubtedly makes the data safer while it travels between your home and the office. Think of the VPN as a pipe within a pipe. The outside pipe is public and the inside pipe is private. The data in the inside pipe is not accessible to the people using the outside pipe. But think of your home computer as the junction between the outside public pipe and the inside private pipe. If someone can access your home computer, they have access to your private pipe, and all of the information flowing between your home computer and the office.

Unfortunately, it's not too hard for the information bandits to get access to your home computer. Let's say your **kids** install a file sharing program for pictures, videos or mp3's for their portable players. These can allow others to gain access to your computer and, quite possibly, the data you are sending to the office. This can compromise the entire system. We all know and control the dangers of spyware and viruses at the office. Chances are your home computer is not as well protected as the system at your office. If you are using your home computer for work, then your corporate

**The sharing software
your kids can't live
without can be used
to gain access to
your home
computer. When you
work at home, you
put your company's
data at risk.**





information can be vulnerable to problems introduced with your children's homework assignments! The home computer can be a weak link in your corporate security chain, especially when children are involved. Just ask yourself and your employees, "how often do the kids go online?"

A VPN and all your corporate protection can be effective security tools, but they are no excuse to let your guard down. When you are out on the road, you drive safely **and** you make sure that everybody is buckled up, right?

4. PASSWORD-PROTECTED FILES KEEP ALL DATA SECURE.

Many popular computer applications offer the ability to "protect" files with passwords. This is designed to prevent unauthorized users from gaining access to that file at a later date. Unfortunately, the system is far from foolproof. The data on the file is 100% accessible to anyone who really wants it. Password security depends on a certain amount of trust. Think of the crossing guard at a school-zone intersection.

Password-protected data is 100% accessible to anyone who really wants it.

Drivers agree to slow down when they see the crossing guard, and the kids agree to obey the crossing guard's commands. But what if just one driver or one pedestrian decides to ignore the crossing guard? The likely result is catastrophe. The people who want your data are not like safe, law-abiding drivers or innocent school children. They are criminals and sociopaths. They do not recognize the implicit agreements that keep the rest of us safe and secure. No mere password will stop them. They cannot be trusted.

In addition, most of us are familiar with functions and resources that allow us to retrieve a lost or forgotten password. Don't you think the data bandits could use this function for more illicit purposes?





5. THE BIGGEST THREAT TO INFORMATION SECURITY IS OUTSIDE HACKERS BREAKING IN, BUT A FIREWALL WILL PROTECT US.

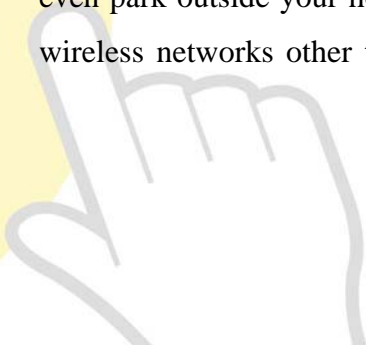
This **must** be true, otherwise why would corporations spend millions of dollars to develop and implement *firewalls* and *security appliances* whose only function is to prevent outside hackers from gaining access to the system? Unfortunately, most security problems start within the organization itself. There are countless risks: a disgruntled employee, a CEO who refuses to remember a **strong password** and instead uses a simple and obvious code, the receptionist who leaves a machine logged on and unattended, employees who share log-in credentials with colleagues, workers who ignore security protocols ... How many of these people do you have in your organization? All it takes is one person acting irresponsibly or with malice to bring down an entire system and cause chaos.

Most security problems start within the organization itself.

6. MY ROUTER AT HOME WAS SET UP BY THE CABLE GUY, SO IT'S SECURE!

It might be. Most cable and DSL operators use equipment designed to protect your privacy. But think of Jim Carey in the movie *The Cable Guy*: would you trust him to install sophisticated, James Bond-like technology such as *encryption devices*? From experience, we know that most home installations are far from safe. Sometimes, the security systems are missing entirely. And did you know that your passwords and other identification codes might be in use on other networks in your area (after all, the same cable guy set those up!), allowing unauthorized users could gain access to your system?

These problems have become so common that many people use their neighbor's Internet service, without the neighbor ever finding out! A passing motorist could even park outside your house and tap into your network from there. I can *see* five wireless networks other than my own, and two of these are completely open. In





other words, there is no telling who might have access to your network, or what they plan to do with it.

7. MY BANK, PAYPAL, AMAZON.COM AND OTHERS ROUTINELY CONFIRM AND SECURE ACCOUNT INFORMATION AND PASSWORDS BY E-MAIL.

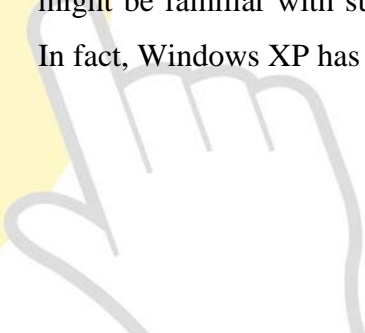
I got an e-mail recently from a vendor telling me I needed to update my **account profile**. There was a convenient link in the e-mail, and the message itself had the vendor's logo and a return address that looked right. I might have assumed that it was safe to click on the link and provide whatever sensitive information the sender requested. This is actually a very common scam called *phishing* (pronounced "fishing"), and it generates millions in ill-gotten profits for the data bandits. Let me be clear: **no legitimate vendor will ever send you an e-mail asking you to confirm sensitive information by clicking on a link**. And never click on a link that comes in such an e-mail. By doing so, you will most certainly be providing someone with your log-in name and password for one of your accounts.

No legitimate vendor will ever ask you to provide sensitive information through an e-mail link.

If you get such an e-mail and you think it might be legitimate, feel free to contact the company directly by some secure channel. Call them. Log in to their website like you normally would. If it is your bank, then take a few minutes to visit the local branch and speak to a teller in person. What seems like a convenient way to do business electronically could actually cost you your information security, and even your identity.

8. I HAVE INTERNET SECURITY SOFTWARE THAT WILL KEEP ME SAFE.

Most new computers come with some security packages already installed. You might be familiar with such programs as *Norton Internet Security* and *ZoneAlarm*. In fact, Windows XP has its own firewall and Windows Vista has built-in protection





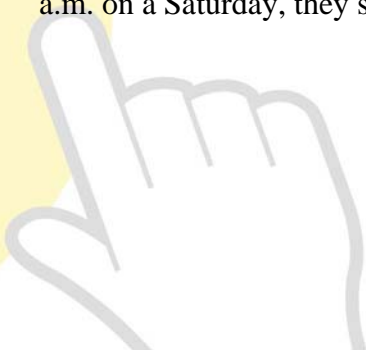
from many common threats. This type of software is designed to monitor your computer's operation and alert you when a problem occurs. But this doesn't mean you can rest easy. Let's face it – we've all been busy and ignored a threat alert. Sometimes it seems that our security devices never stop. They're like Chicken Little telling us the sky is falling. Often they warn us about things that actually pose no danger whatsoever.

You cannot expect your security software to do all the work. You have to spend some time configuring the software so it picks up only the real threats and doesn't waste your time or its own energy scanning potential threats that are actually valid and required functions. Many people get so annoyed that they eventually turn off the security functions completely. This is understandable, but remember: **if you turn off your security programs, you will no longer be protected.** New security threats come online every day, and even the best security packages need to be updated on a regular basis. This is typically done automatically by the manufacturer. It is up to you, however, to make sure that you have the latest version installed on your computer.

New security threats come online every day, and even the best security packages need to be updated on a regular basis.

9. IT'S GREAT THAT MY STAFF IS WILLING TO WORK FROM HOME OR STARBUCKS!

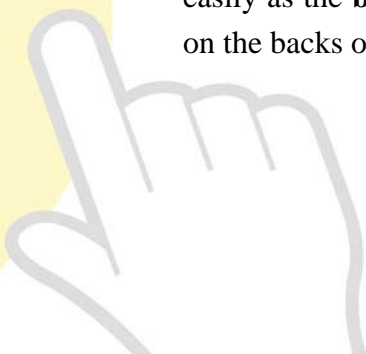
It seems like everybody is working longer and harder these days. Laptop computers, cell phones and other modern marvels have given us unprecedented mobility and productivity. And it is true that people work best on their own schedule, striking while the iron is hot. Great ideas don't just happen during office hours. So if the staff wants to take data with them, or go online and **produce** at 1 a.m. on a Saturday, they should be encouraged to do so. It might pay big dividends.





It also adds significant risk to your operations. The environment in which they are burning the midnight oil is beyond your control. Here are just **some** of the most common risks associated with working off-site:

- Files containing your data might be exposed on open WiFi networks like tMobile at Starbucks, FlyPittsburgh Wireless or that hotel's wireless network. There are so many others, it is impossible to list them all. To paraphrase the old public service announcement, when you log on to a wireless network, you are logging on to every computer on that network.
- Someone might just peer over the user's shoulder and "notice" some confidential information on the screen. Remember that kid who copied the answers off your sixth-grade math test? He's grown up now and is working for the competition.
- We've all known or heard of someone who has had a laptop containing vital information stolen from a car or left one behind on an airplane. What about your Treo / Palm / Blackberry? Any confidential information on those devices? Could your organization recover from such a catastrophic loss and the resulting damage to your reputation?
- One of our clients reported that an employee, generous to a fault, had loaned a company laptop to a friend who was writing a thesis paper. Let's say that the friend is a computer novice who accidentally deletes several important files. Or how about this nightmare scenario: the friend decides to pick up some quick cash for next semester's tuition. How long would it take him to make copies of all the files and pass them along to your biggest competitor?
- Remember that most off-site locations are not nearly as well protected against viruses as your own office. While you're relaxing at Starbucks, you might pick up something to go along with that double-mocha-latte. Computer viruses can be carried into your office on laptops, just as easily as the **bubonic plague bacillus** was carried into medieval Europe on the backs of rats traveling on trading ships.





We are certainly not suggesting that workers should be prevented from working off-site or after hours. That is simply not practical in the modern business environment, where productivity and creativity are paramount. Still, you must exercise extreme caution. Sometimes it is not a bad idea to be just a little paranoid (and teach your people to be paranoid). Remember, everyone *is* out to get you. You CAN protect your valuable information resources, but when they leave the office, the work required to do so increases exponentially.

10. MY COMPUTER NEVER LEAVES THE OFFICE (OR HOUSE OR SHOP ...) SO THE INFORMATION ON IT IS SAFE.

It is a troubling question, but just how safe is your office, or your house, or your shop? There are cleaning people and “security” personnel in your office at night when no one else is around. Who hired these people, and who is checking their credentials? There might be repairmen crawling around your house right now. How well do you know them? What happens if a burglar breaks in while you are away on a well-earned vacation, or worse, you take your computer along with you and some hotel maid decides to stash it in her laundry cart? In any of these scenarios, your data is gone, along with your money, your time, your reputation and everything else you’ve worked for your entire life. Let’s face it, **the information you have on your computer might be worth more to some people than their annual salary.** Your best defense is to take every possible precaution to safeguard your computer when you are away from it, or even if you just have your back turned. Information security is a 24-7-365 concern.

In conclusion ...

Cyberspace is an exciting new frontier, but just as wild and untamed as Dodge City at the end of a cattle drive. Unlike the innocent townfolk in every old John Wayne movie, however, you can’t simply dive into a rain barrel once the gunfight

**You have to
protect yourself,
and the best way
to start is by
facing the cold,
hard facts about
information
security.**



starts. You have to protect yourself, and the best way to start is by facing the cold, hard facts about information security: passwords offer little protection against determined hackers; e-mails can be intercepted and read by just about anyone; Virtual Private Networks are anything but private; firewalls are of little use because the greatest threats to your organization are found within the four walls of your own office; security systems installed by people who earn extra money by selling you HBO cannot be entirely trusted; criminals have a knack for impersonation and can make you think you're sharing information with your bank when you're really giving away vital financial and personal information; Internet security software is only as good as the last virus it detected; laptops have a way of disappearing, along with your critical data; and, finally, nowhere is completely safe.

Truth ... or consequences

These are difficult issues, and no one wants to dwell on the negative. Once you accept reality, however, you will be much better prepared to protect your data, your business, yourself and your family.

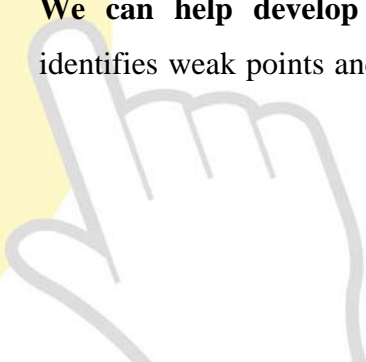
Help is on the way

OK, you say, I'm losing sleep now. Please do something! Rest easy. We at interpret.co can help:

We can conduct a rigorous and thorough Information Security Assessment.

We will look at every machine that touches your data, and every location where that machine is used. We will examine the connectivity and technology that you use to communicate information and the ways you store and archive information. Consider this the white-glove test for information security.

We can help develop and implement an Information Security Plan that identifies weak points and provides greater security throughout your system. Does





your vehicle have LoJack? We can install a similar device that will trace stolen laptops. We can even help you come up with passwords that will frustrate the most determined information bandits. And we can help you find other ways of sharing data, so you don't have to post your most sensitive e-mail messages on a great big electronic party line.

The situation is scary, but not hopeless. Just don't let your guard down. Watch in the upcoming weeks for our tips and solutions on how to navigate around these issues. If you would like the PDF version (or hard copy) of this special report to pass on to your friends and colleagues, we would be happy to send it to you. Also, if you are interested in our "Quick Tips" to help you address each of the 10 myths, please contact us.

For more information, contact:

Daniel H. Harris
Principal en-terpretor
773-868-4381 Phone
773-913-6217 eFAX
dharris@en-terpret.com
Translating Technology in Solutions

